

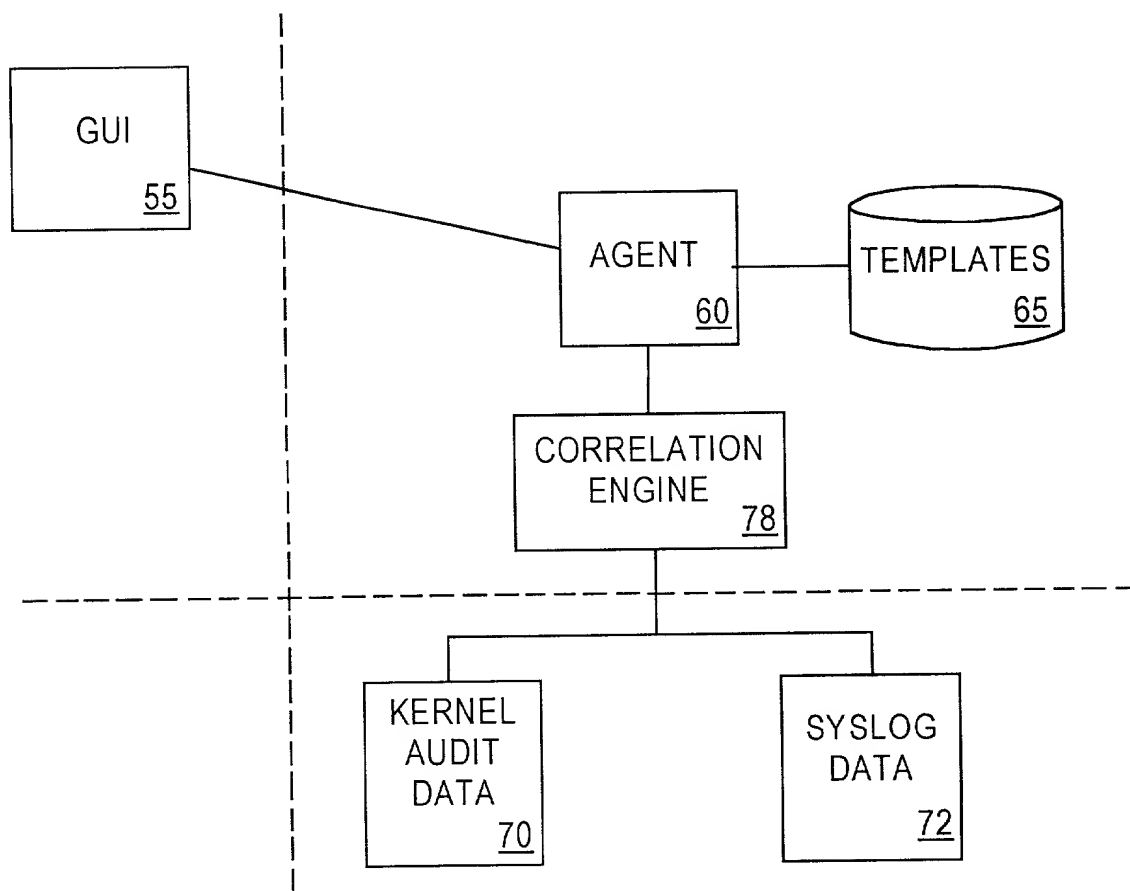
COMPUTER ARCHITECTURE FOR AN INTRUSION DETECTION SYSTEM

S.N. 09/878,320

Inventor: Mark Crosbie, et al.

Docket No. 10012170-1

FIG. 1



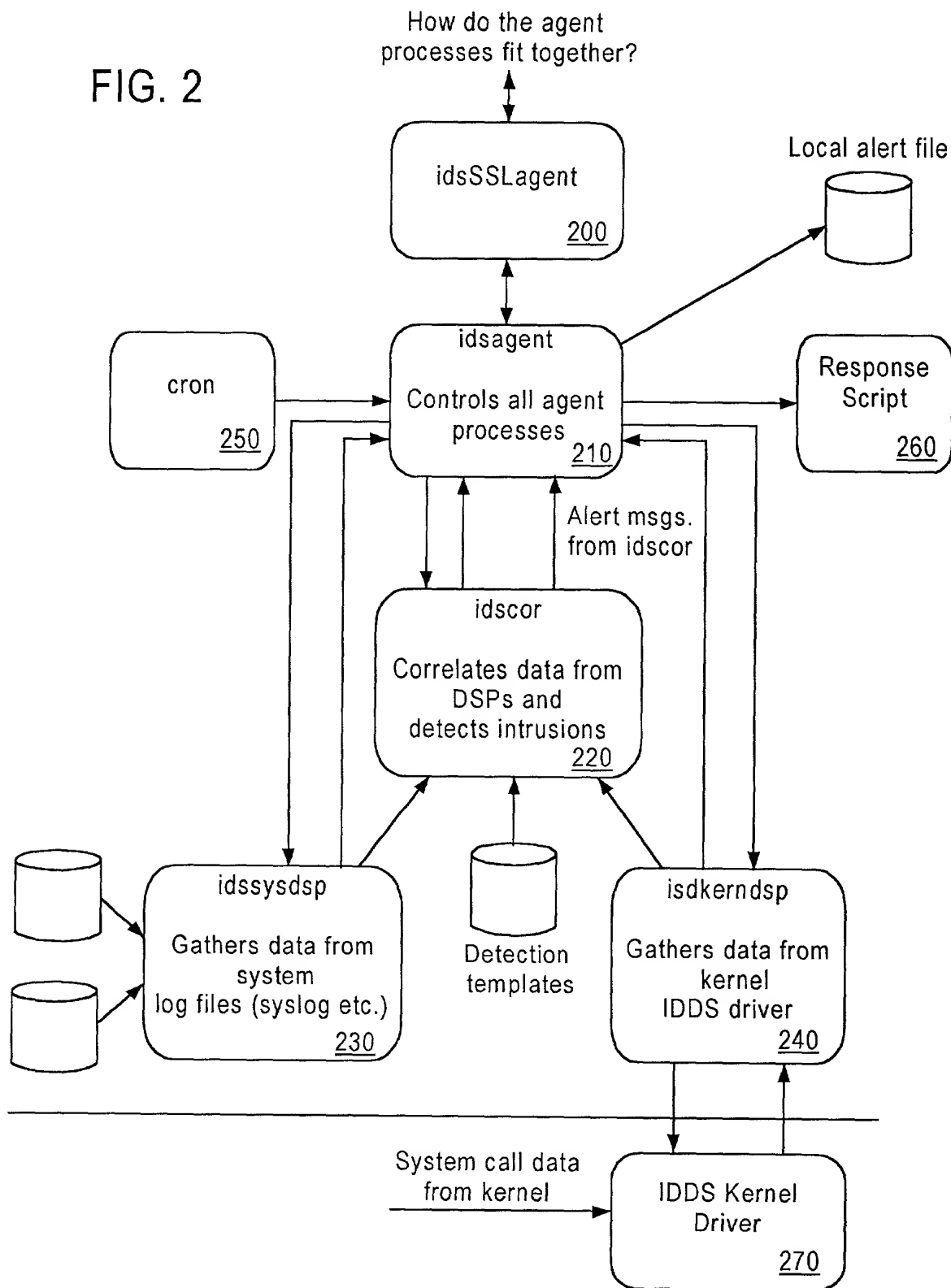
COMPUTER ARCHITECTURE FOR AN INTRUSION DETECTION SYSTEM

S.N. 09/878,320

Inventor: Mark Crosbie, et al.

Docket No. 10012170-1

FIG. 2



COMPUTER ARCHITECTURE FOR AN INTRUSION DETECTION SYSTEM

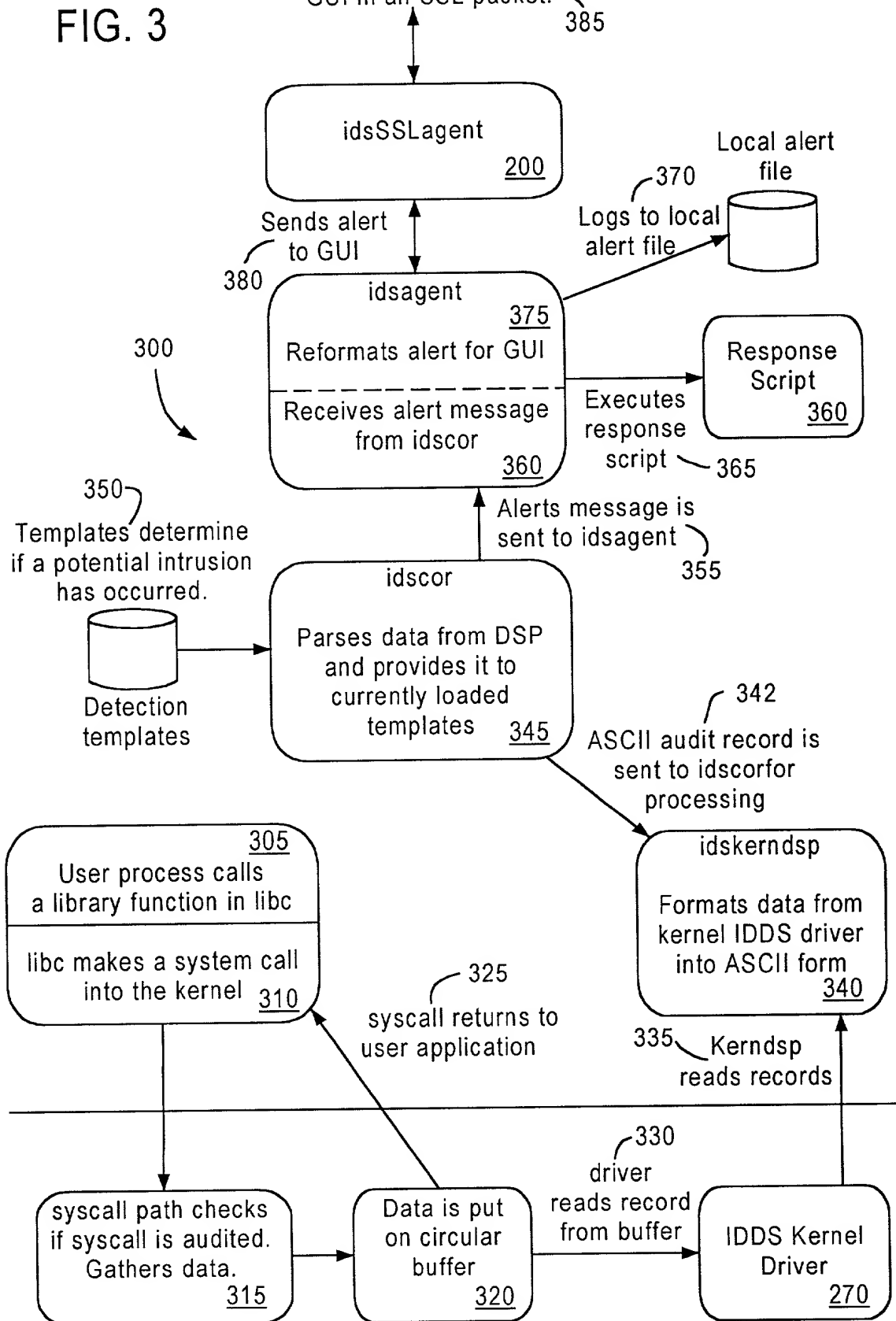
S.N. 09/878,320

Inventor: Mark Crosbie, et al.

Docket No. 10012170-1

Alert text is sent to GUI in an SSL packet.

FIG. 3



[illegible]

Inventor: Mark Crosbie, et al.
Docket No. 10012170-1



- Agent Monitor
- Remote connection

- Installation
- Initialization
- Configuration
- Control/Status

- ECS engine core
- Circuit/data control modules
- Messaging control
- Status/Error/Trace output
- Command input and dispatch
- Engine state dump

- Audit
- Syslog
- Network

- Kernel patterns
- Network patterns (future)
- Web server patterns (from logs)

[illegible][illegible][illegible][illegible]